IN THE CLAIMS:

Claim 1 (Original): A method for enabling a user to access a restricted area via biometric authentication, the method comprising:

receiving a portion of user information used to enable the user to access the restricted area, said information presented by a system operator;

storing, in a database, in association with an identification code said portion of user information as a partially enabled user record;

communicating the identification code to the user;

receiving, at a system point of access, a record enablement request, said request including the identification code and a user biometric sample; and

storing the user biometric sample with said user record.

Claim 2 (Original): The method of claim 1, further comprising marking said user record as active.

Claim 3 (Original): The method of claim 1, further comprising granting the user access to the restricted area.

Claim 4 (Original): The method of claim 3, wherein access to the restricted area provides access to a restricted activity.

Claim 5 (Original): The method of claim 1, wherein the enablement request further includes a user system identification number used in conjunction with the user biometric to identify the user.

Claim 6 (Original): The method of claim 1, wherein the identification code associated with the user record is chosen by the system operator.

Claim 7 (Currently Amended): The method of claim 1, wherein <u>the identification code is digitally read.</u>

Claim 8 (Canceled).

Claim 9 (Original): The method of claim 7, wherein the identification code is digitally read from a token.

Claim 10 (Original): The method of claim 7, wherein the identification code is digitally read from an electronic device.

Claim 11 (Currently Amended): The method of claim [9] <u>10</u>, wherein the identification code is a device system registration code.

Claim 12 (Original): The method of claim 1, wherein the identification code is automatically communicated to the user.

Claim 13 (Original): The method of claim 1, further comprising the system operator associating access parameters with said user record.

Claim 14 (Currently Amended): The method of claim [12] <u>13</u>, wherein the access parameters determine the manner in which the user accesses the restricted area.

Claim 15 (Currently Amended): The method of claim [12] <u>13</u>, wherein the access parameters include regulating one or more of the time the user is allowed to enable said user record, the user access frequency once the user record is enabled, one or more points of access the user may use

to enable said user record, and one or more points of access the user may use to access the restricted area.

Claim 16 (Currently Amended): The method of claim [12] 13, wherein the system operator associates one or more access parameters with a plurality of user records.

Claim 17 (Original): The method of claim 1, wherein the restricted area is an area of virtual space in a network.

Claim 18 (Original): The method of claim 1, further comprising:

receiving, at the database, a system operator biometric sample;

determining, at said system database, if the system operator biometric sample matches a system operator biometric record stored in the database; and

if the system operator biometric sample matches a biometric record stored in the database, allowing the system operator access to present said portion of user information.

Claim 19 (Original): The method of claim 1, further comprising associating one or more managing privileges with said user record.

Claim 20 (Currently Amended): The method of claim [18] 19, wherein said managing privileges include allowing the user to partially enable one or more other users to access the restricted area.

Claim 21 (Currently Amended): The method of claim [19] 20, wherein the system operator must approve said partial enablement conducted by the user with managing privileges of one or more other users before allowing enablement.

Claim 22 (Original): The method of claim 1, further comprising:

displaying, at the point of access, a portion of user information stored as said user record at the database;

prompting the user to confirm said displayed information; and

storing the confirmation presented by the user at the database.

Claim 23 (Currently Amended): The method of claim [21] 22, wherein if a portion of said displayed information is incorrect, the user is provided with an opportunity to present the correct information.

Claim 24 (Original): The method of claim 1, wherein said point of access includes a record output device for outputting one or more records, the records being configured as one or more of a printed report, a media output to an electronic device, and an email.

Claim 25 (Currently Amended): The method of claim [23] 24, wherein the record output includes one or more of the data entered during the system access, the data necessary to enable the user, the date of access, and the time of access.

Claim 26 (Original): The method of claim 1, wherein the system operator is provided with one or more of a record output of the user information stored in said system database and a record output of the identification code associated with said user record.

Claim 27 (Currently Amended): The method of claim [25] 26, wherein said record output is configured as one or more of a printed report, a media output it an electronic device and an email.

Claim 28 (Currently Amended): The method of claim [26] 27, wherein said record output is communicated to the user.

Claim 29 (Currently Amended): The method of claim [27] 28, wherein said record output is communicated to the user automatically by the database.

Claim 30 (Original): A method for enabling a system operator to pre-enroll users within a system for biometric authentication, the method comprising:

receiving, from the system operator, defined access rights for a user of the biometric authentication system;

storing said defined access rights in association with an identification code as a partially enabled user record; and

communicating said identification code to the user, said identification code enabling said user to activate said user record through the provision of a biometric sample.

Claim 31 (Currently Amended): The method of claim [29] 30, further comprising:

receiving, at a point of enablement, said identification code;

receiving, at the point of enablement, a user biometric sample;

determining if said identification code matches at least one identification code stored in the database;

if said identification code matches at least one identification code stored in the database, storing in the user record associated with said identification code the biometric sample; and

marking, said user record as active.

Claim 32 (Currently Amended): The method of claim [30] 31, wherein said point of enablement is co-located with a point of allowance.

Claim 33 (Currently Amended): The method of claim [30] 31, wherein the system operator can revoke said user record for any reason.

Claim 34 (Currently Amended): The method of claim [30] 31, further comprising:

receiving, at the point of allowance, an activity request from the user; and

accepting said activity request if it meets the parameters associated with said user record.

Claim 35 (Currently Amended): The method of claim [33] 34, wherein said activity request further comprises the user presenting a biometric sample and wherein that biometric sample is matched to a biometric record at the point of allowance.

Claim 36 (Currently Amended): The method of claim [33] 34, wherein said activity request further comprises the user presenting a biometric sample and wherein that biometric sample is matched to a biometric record at a central location.

Claim 37 (Currently Amended): The method of claim [33] 34, further comprising at least one biometrically authorized financial transaction.

Claim 38 (Currently Amended): The method of claim [30] 32, further comprising:

receiving, at the point of allowance, an activity request from the user;

determining if said activity request meets the parameters stored in association with said user record;

if said activity request does not meet the parameters stored in association with said user record, initiating a system override;

notifying the system operator of said system override;

providing the system operator an opportunity to provide approval of said system override; and

accepting, at the point of allowance, said activity request if the system operator approves said initiated system override.

Claim 39 (Currently Amended): The method of claim [29] 30, wherein said portion of the user information is pulled from a third party database.

Claim 40 (Original): A method for partially enabling a plurality of users to access a restricted area via biometric authentication, the method comprising:

receiving, at a system database in a biometric verification network, a plurality of portions of user information used to enable a plurality of users to access said area;

storing said portions of user information as a plurality of partially enabled user records;

generating, at the system database, a plurality of identification codes, each code uniquely associated with a user record selected from a plurality of user records; and

communicating said identification codes to the respective users.

Claim 41 (Currently Amended): The method of claim [39] 40, further comprising:

receiving, at a system point of access, an identification code, said identification code presented by one of said plurality of users;

receiving at said system point of access, a biometric sample, said biometric sample presented by said one of said plurality of users;

storing, at the system database, said user biometric sample; and

marking said user record as enabled to access the system.

Claim 42 (Original): A method in a biometric system for enabling a user to access a restricted area, the method comprising:

pre-enrolling a user in the biometric system by storing a portion of a required amount of user record information in a database, said portion of required user record information including defined access rights to the restricted area;

receiving an enrollment completion request from the user, said enrollment completion request including an identification code associated with said user record and a user biometric sample;

storing said user biometric sample in said user record; and

marking said user record as an active user record.

Claim 43 (Currently Amended): The method of claim [41] 42, further comprising generating said identification code and communicating said generated identification code to said user after pre-enrollment is complete.

Claim 44 (Original): A method in a biometric system for enabling a user to access a restricted area, the method comprising:

associating an identification code with an inactive user record, said inactive user record requiring input from a user for activation of said user record;

receiving an request from the user, said activation request including said identification code and biometric sample from the user; and

activating said user record upon storage of said biometric sample in said user record.

Claim 45 (Currently Amended): The method of claim [43] 44, wherein said inactive user record includes access rights definitions.

Claim 46 (Original): A method for controlling access to a restricted area, the method comprising:

defining individual access rights to the restricted area for each of a plurality of users;

storing said defined individual access rights in a respective plurality of user records, each of the plurality of user records having a unique identification code associated therewith;

distributing said plurality of unique identification codes to said plurality of users;